

Estimados profesionales de las comunicaciones:

Escribimos en nombre de un grupo internacional de Agencias gubernamentales de todo el Mundo al objeto de solicitar que su organización se sume a una iniciativa internacional que trata de evitar que los *spammers* (personas que envían spam o correo basura) comprometan la seguridad de los ordenadores de los usuarios de Internet, utilizándolos como “*spam zombies*” (emisores de *spam* encubiertos).

Nuestras Agencias son las responsables de la lucha contra el spam mediante el cumplimiento de la normativa vigente, investigación técnica, concienciación y aspectos educacionales, desarrollo de políticas y alianzas publico-privadas.

Los *spammers* utilizan los ordenadores personales ubicados en los hogares de los usuarios para enviar correos electrónicos de forma masiva, convirtiendo a estos en servidores de correo aprovechando debilidades y fallos de seguridad. De este modo, utilizando los *spam zombies*, oscurecen el verdadero origen de los mensajes masivos enviados.

Como Proveedora de Servicios de Internet, a su organización le interesa preservar la integridad del sistema de correo electrónico, que se encuentra amenazado por el ataque del *spam* a través de los mencionados *zombies*. Además, los receptores pueden culpar a su organización por el spam que parece haber sido originado desde sus sistemas, o desde los sistemas de sus usuarios. Por otro lado, el spam puede sobrecargar sus redes incrementando los costes administrativos.

Le animamos a implementar estas medidas voluntarias contra los *zombies*, si todavía no las ha adoptado ¹

- Bloquee el Puerto 25 excepto en los casos en los que se requiera tráfico SMTP saliente para usuarios de servidores destinados al trafico de clientes. Explore la posibilidad de implementar SMTP autenticado en el puerto 587 para clientes que deben operar con servidores de correo saliente.
- Aplique controles de tasas límites de tráfico para *relays* de correo electrónico
- Identifique los ordenadores que estén emitiendo cantidades atípicas de correo, y tome medidas para determinar si el ordenador está actuando como un *zombie* emisor de *spam*. Cuando sea necesario, ponga en cuarentena el ordenador afectado hasta que el origen del problema sea eliminado.
- Ofrezca a sus clientes consejos en lenguaje sencillo sobre como prevenir que sus ordenadores queden infectados por virus informáticos (gusanos, troyanos, y otros programas) que pueden convertir sus ordenadores personales en *zombies* emisores de *spam*, y provéalos de la asistencia y herramientas adecuadas.
- Provea o recomiende a sus clientes la utilización de herramientas fáciles de usar para eliminar los *zombies* si sus ordenadores han sido ya infectados, y facilíteles la asistencia apropiada para ello.

Finalmente, además de animar a los Proveedores de Servicio de Internet a prevenir que los *spammers* creen ordenadores *zombies*, estamos desarrollando un plan para identificar direcciones IP de posibles ordenadores *zombies* en todo el Mundo, así como los Proveedores de Servicio de Internet y otros proveedores de servicios de conectividad de Internet que parecen ser responsables de las direcciones IP afectadas. Este análisis tendrá su base en información compilada de fuentes publicas tales como bases de datos de *spam* y *Whois*. Existe la intención de establecer contacto por carta con los proveedores asociados a las direcciones IP utilizadas por posibles “*spam zombies*”. Esta segunda carta pedirá que los proveedores involucrados incrementen sus esfuerzos para solucionar problemas relacionados con *zombies* instalados en sus sistemas.

Para mas información sobre este proyecto, así como para visualizar una lista de Agencias asociadas en este esfuerzo, visite www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm.

Muchas gracias por su asistencia en la lucha contra el *spam*.

1) Si pone en práctica estas recomendaciones, por favor, asegúrese que no entran en conflicto con leyes existentes en su jurisdicción, tales como aquellas relativas a Protección de Datos, o leyes sobre la confidencialidad, intimidad o seguridad de la Información, u otros requerimientos u obligaciones legales. Tener en cuenta que estas recomendaciones pueden ser obligatorias en algunas jurisdicciones.